

GeniusQ – Lernplattform

Auftragsverarbeitungsvereinbarung (AVV)

Stand: 13.08.2026

Vertragsparteien

Diese Auftragsverarbeitungsvereinbarung (AVV) wird geschlossen zwischen

dem Auftraggeber – dem jeweiligen Firmenkunden (Arbeitgeber), der die Lernplattform GeniusQ für seine Beschäftigten nutzt; die Angaben ergeben sich aus dem zugrunde liegenden Hauptvertrag –
und

dem Auftragnehmer

**Steinbeis Transferzentrum für Angewandte Künstliche Intelligenz Prof. Dr. Oliver Janz in
Trägerschaft der Transfer GmbH der Dualen Hochschule Baden-Württemberg** Im Alten Graben 19
64673 Zwingenberg E-Mail: oliver.janz@stw.de

– Betreiber der Lernplattform GeniusQ, im Folgenden „Auftragnehmer“ –

1. Gegenstand und Dauer der Verarbeitung

Der Auftraggeber nutzt die vom Auftragnehmer betriebene Lernplattform GeniusQ. Sie wird auf Infrastruktur in Deutschland betrieben; die Datenbank wird als Managed-Service in derselben Region bereitgestellt. Die Auslieferung von Medien- und statischen Inhalten aus dem Object Storage erfolgt über ein Content Delivery Network mit Sitz in der EU. Die Plattform ermöglicht den Lernenden, Trainern und Administratoren des Auftraggebers das Erstellen, Durchführen und Nutzen von Onlinekursen. KI-Funktionen werden über Programmierschnittstellen der hierfür eingesetzten Anbieter bereitgestellt; die Inferenz der Anthropic-Modelle erfolgt ausschließlich innerhalb der EU (Region eu-central-1, Frankfurt). Die namentliche Benennung der eingesetzten Dienstleister – mit Zweck, Standort und Nachweis – erfolgt in der Anlage „Liste der Unterauftragsverarbeiter“ (Ziffer 8) in ihrer jeweils geltenden Fassung. Ein Wechsel der dort geführten Anbieter richtet sich nach dem Verfahren der Ziffer 8 und ändert diese Vereinbarung nicht. Diese Vereinbarung gilt für die Dauer der Nutzung der Plattform durch den Auftraggeber.

2. Art und Zweck der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zu folgenden Zwecken: * Bereitstellung und Betrieb der Lernplattform * Benutzerverwaltung, Rollen und Kurszuordnung * Durchführung von Onlinekursen * Protokollierung des Lernfortschritts * Technischer Betrieb, Wartung und Sicherheit * Keine Verarbeitung zu eigenen Zwecken.

Der Auftragnehmer ist berechtigt, personenbezogene Daten zu anonymisieren. Anonymisierte Daten (bei denen kein Rückschluss auf einzelne Personen mehr möglich ist) unterliegen nicht mehr der Weisungsgebundenheit und dürfen vom Auftragnehmer zur Verbesserung der Systemstabilität, für statistische Auswertungen und zur Weiterentwicklung der Lernplattform zeitlich unbegrenzt genutzt werden. Eine Nutzung anonymisierter Daten zum Training externer KI-Modelle erfolgt nicht.

3. Nutzung von KI-Funktionen

Die Plattform stellt KI-gestützte Funktionen bereit, die auf zwei Arten genutzt werden können: *

Erstellung von Lerninhalten: Unterstützung von Trainern und Administratoren bei der Erstellung, Strukturierung und Analyse von Lehrmaterialien. * **Lernunterstützung:** Interaktive Funktionen für Lernende (z. B. Beantwortung von Fragen, Feedback zu Aufgaben, Prüfungssimulationen).

Für beide Anwendungsbereiche gilt: * **Übermittlung zur Vertragserfüllung:** Inhalte, die Nutzer in KI-Funktionen eingeben (z. B. PDF-Dokumente, Freitextantworten), werden an die in der Anlage „Liste der Unterauftragsverarbeiter“ geführten KI-Dienstleister übermittelt. Dies umfasst auch die optische

Zeichenerkennung (OCR) und das Parsing hochgeladener Dokumente, die Umrechnung von Texten in Vektordarstellungen für die Suche sowie die Sprachausgabe auf Anforderung eines Nutzers. *

Mandantenbezogene Modellfreigabe: Für den Dialog mit Lernenden kann je Auftraggeber festgelegt werden, welche Sprachmodelle verwendet werden dürfen. Die Freigabe wird zur Laufzeit bei jeder Anfrage geprüft. * Dies erfolgt ausschließlich weisungsgebunden zum Zweck der Analyse und der Generierung von Antworten. * **Kein KI-Training:** Der Auftragnehmer sichert zu, dass die übermittelten Kundendaten gemäß den Vereinbarungen mit den KI-Anbietern nicht zum Training oder zur Verbesserung der KI-Modelle der Anbieter verwendet werden. * Die Daten bleiben vertraulich und isoliert. * **Datenminimierung:** Der Auftragnehmer implementiert technische Maßnahmen, um die Übermittlung personenbezogener Metadaten (wie User-IDs, Klarnamen) an KI-Dienste auf das technisch notwendige Minimum zu beschränken.

4. Art der personenbezogenen Daten

- Stammdaten: Name, geschäftliche E-Mail-Adresse, Rollen
- Logindaten, Hashwerte, interne IDs
- Kursdaten, Lernstände, Kommentare, Uploads
- Nutzungsdaten (Zeitpunkte, Interaktionen)
- Inhalte, die Nutzer in KI-Funktionen eingeben

4a. Ausschluss besonderer Datenkategorien

Die Plattform ist nicht für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO (z. B. Gesundheitsdaten, politische Meinungen, religiöse Überzeugungen) und nicht für die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten im Sinne von Art. 10 DSGVO konzipiert. Gleiches gilt für Gesundheits- und Bewerberdaten sowie für Daten, die einem besonderen Berufsgeheimnis (§ 203 StGB) unterliegen. Der Auftraggeber verpflichtet sich, keine Kursinhalte oder Eingabefelder bereitzustellen, die systematisch zur Erhebung solcher Daten führen. Sollte der Auftraggeber dennoch besondere Kategorien verarbeiten wollen, ist vorab eine gesonderte Vereinbarung zu treffen.

5. Kategorien betroffener Personen

- Lernende des Auftraggebers – je nach Auftraggeber etwa Beschäftigte, Auszubildende, Studierende oder Teilnehmende an Weiterbildungsangeboten
- Trainer, Dozenten und Lehrende des Auftraggebers, einschließlich der von ihm hierfür beauftragten Personen
- Administratoren des Auftraggebers
- Personen, die einen Lernbaustein über eine in ein Fremdsystem eingebettete Komponente ohne persönliche Anmeldung nutzen; diese werden ausschließlich unter einem Pseudonym geführt (Ziffer 12.5)

6. Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich: * Daten nur auf dokumentierte Weisung zu verarbeiten. * DSGVO-Vorgaben einzuhalten (insbesondere Art. 28). * Vertraulichkeit sicherzustellen. * Geeignete technische und organisatorische Maßnahmen umzusetzen. * Den Auftraggeber bei Datenschutzpflichten zu unterstützen. * Daten nach Vertragsende zu löschen oder zu übergeben. * Datenschutzverletzungen unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Kenntniserlangung, zu melden.

7. Pflichten des Auftraggebers

- Sicherstellung der Rechtmäßigkeit der Verarbeitung
- Information des Auftragnehmers über relevante Änderungen
- Sichere Verwaltung von Nutzerkonten und Rollen
- Nutzung der Plattform im gesetzlichen Rahmen

8. Unterauftragsverarbeiter

Genehmigte Unterauftragsverarbeiter: Die zum Zeitpunkt des Vertragsschlusses vom Auftraggeber genehmigten Unterauftragsverarbeiter sowie deren Standorte und Aufgaben sind in der **Anlage „Liste der Unterauftragsverarbeiter“** aufgeführt.

Vertragliche Grundlagen: Mit allen Unterauftragsverarbeitern bestehen Auftragsverarbeitungsverträge oder gleichwertige vertragliche Vereinbarungen gemäß Art. 28 DSGVO. Der Auftragnehmer prüft bei wesentlichen Änderungen der Vereinbarungen, ob das Datenschutzniveau gewahrt bleibt.

Änderungsmechanismus und Einspruch: Der Auftragnehmer ist berechtigt, die in der Anlage aufgeführten Unterauftragsverarbeiter zu ändern (neue hinzuzuziehen oder bestehende zu ersetzen), sofern das vertraglich vereinbarte Datenschutzniveau gewahrt bleibt.

Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen in Textform (z. B. per E-Mail oder Systembenachrichtigung). Diese Information erfolgt mit einer Vorlaufzeit von mindestens **14 Tagen** vor dem geplanten Einsatz des neuen Unterauftragsverarbeiters.

Genehmigungsfiktion: Der Auftraggeber kann gegen die Änderung innerhalb der 14-tägigen Frist ab Zugang der Information aus wichtigem datenschutzrechtlichem Grund Einspruch einlegen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Änderung als genehmigt.

Im Fall eines begründeten Einspruchs werden die Parteien eine einvernehmliche Lösung suchen. Gelingt dies nicht, steht dem Auftragnehmer ein Sonderkündigungsrecht zu, sofern die Leistung ohne den neuen Unterauftragsverarbeiter nicht erbracht werden kann.

9. Datenübermittlung in Drittländern

1. Das Hosting der Plattform einschließlich Datenbank, Object Storage und Vektordatenbank erfolgt ausschließlich in Deutschland. Auch die Speicherung der verschlüsselten Datensicherungen erfolgt ausschließlich in Deutschland.
2. Die Auslieferung von Medien- und statischen Inhalten erfolgt über ein Content Delivery Network mit Sitz in der EU. Die eingesetzte Zone ist auf europäische Edge-Server beschränkt; die Auslieferung einschließlich der dabei verarbeiteten technischen Verbindungsdaten (insb. IP-Adressen der abrufenden Nutzer) erfolgt ausschließlich innerhalb der EU/des EWR. Eine Übermittlung in ein Drittland findet hierbei nicht statt.
3. Die KI-Inferenz der Anthropic-Modelle erfolgt ausschließlich innerhalb der EU (Region eu-central-1, Frankfurt); eine Übermittlung an die Anthropic PBC (USA) findet hierbei nicht statt.
4. Eine Übermittlung in ein Drittland erfolgt ausschließlich gegenüber denjenigen Dienstleistern, die in der Anlage „Liste der Unterauftragsverarbeiter“ mit einem Standort außerhalb der EU/des EWR ausgewiesen sind. Der Auftragnehmer stellt die Zulässigkeit durch geeignete Garantien gem. Art. 44 ff. DSGVO sicher.
5. Rechtsgrundlage für diese Übermittlungen sind vorrangig der Angemessenheitsbeschluss für das EU-US Data Privacy Framework (DPF), sofern der Anbieter zertifiziert ist.
6. Ersatzweise oder ergänzend werden die EU-Standardvertragsklauseln (SCC) abgeschlossen.
7. Sollte ein Unterauftragsverarbeiter seine Zertifizierung unter dem EU-US Data Privacy Framework verlieren oder sollte der Angemessenheitsbeschluss aufgehoben werden, stellt der Auftragnehmer die Rechtmäßigkeit der Datenübermittlung durch den Abschluss von EU-Standardvertragsklauseln (SCC) oder vergleichbare geeignete Garantien sicher.

10. Unterstützungspflichten und Übermittlung personenbezogener Lerndaten

Der Auftragnehmer verarbeitet personenbezogene Lerndaten (z. B. Lernfortschritte, Kursteilnahmen, Testergebnisse) ausschließlich im Auftrag des Auftraggebers. Der Auftragnehmer ist berechtigt und verpflichtet, dem Auftraggeber sämtliche personenbezogenen Lerndaten zur Verfügung zu stellen, die für die Nutzung der Plattform erforderlich sind. Dies umfasst insbesondere Informationen darüber, ob Nutzer Kurse begonnen, abgeschlossen oder Tests bestanden bzw. nicht bestanden haben. Eine Weitergabe personenbezogener Lerndaten an andere Stellen als den Auftraggeber erfolgt nicht. Der Auftraggeber ist dafür verantwortlich, seine Nutzer gemäß Art. 13 DSGVO über die Verarbeitung und Auswertung der Lerndaten zu informieren. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Datenschutzpflichten, insbesondere bei: * Auskunftersuchen betroffener Personen, * Berichtigung, Einschränkung und Löschung personenbezogener Daten, * Bereitstellung von Daten für Zwecke der Datenübertragbarkeit, * Meldung und Dokumentation von Datenschutzverletzungen, *

11. Technische und organisatorische Maßnahmen (TOM)

Die technischen und organisatorischen Maßnahmen sind in Anhang 1 (TOM-Dokument) beschrieben und Bestandteil dieser Vereinbarung. Der Auftragnehmer ist berechtigt, diesen Anhang bei gleichbleibendem Schutzniveau zu aktualisieren.

12. Löschung, Rückgabe und Aufbewahrung von Daten

Nach Vertragsende gelten folgende Regelungen:

12.1 Löschung personenbezogener Daten Der Auftragnehmer löscht sämtliche personenbezogenen Daten unverzüglich, spätestens innerhalb von 7 Werktagen nach Beendigung des Vertragsverhältnisses, sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

12.2 Gesetzliche Aufbewahrungspflichten Der Auftragnehmer ist nur dann zur Aufbewahrung verpflichtet, wenn dies gesetzlich vorgeschrieben ist (z. B. handels- oder steuerrechtliche Aufbewahrungsfristen nach HGB/AO). Da der Auftragnehmer keine abrechnungsrelevanten Unterlagen der Nutzer speichert, bestehen im Regelfall keine gesetzlichen Aufbewahrungspflichten für personenbezogene Lerndaten. System- und Sicherheitsprotokolle (z. B. ServerLogs) können personenbezogene Daten wie IPAdressen enthalten. Diese werden ausschließlich zur Sicherstellung der Systemstabilität genutzt und unterliegen folgenden Fristen: * AccessLogs: automatische Löschung nach maximal 30 Tagen * Fehler- und Ereignisprotokolle: automatische Löschung nach maximal 90 Tagen Längere Aufbewahrung erfolgt nur, wenn dies zur Aufklärung sicherheitsrelevanter Vorfälle erforderlich ist.

12.3 Rückgabe der Daten Auf Wunsch des Auftraggebers stellt der Auftragnehmer vor der Löschung eine vollständige Kopie personenbezogener Daten in einem gängigen, strukturierten Format bereit.

12.4 Umgang mit Backups Backups enthalten personenbezogene Daten und werden wie folgt behandelt: * Eigene Backups des Auftragnehmers * Backups umfassen sämtliche Datenbestände, die personenbezogene Daten enthalten können (Datenbank, Object Storage, Vektordatenbank, Betriebskonfiguration). * Backups werden mindestens täglich erstellt, die Datenbank alle 6 Stunden. * Backups werden bereits vor der Übertragung clientseitig verschlüsselt und bei einem zweiten Anbieter in Deutschland gespeichert; dieser hat zu keinem Zeitpunkt Zugriff auf Klartextdaten. * Backups werden nach 14 Tagen automatisch überschrieben. * Damit werden personenbezogene Daten nach Ablauf der Backup-Rotation endgültig entfernt. * Backups des Unterauftragsverarbeiters, der die Managed-Datenbank betreibt (in der Anlage geführt) * Dieser erstellt im Rahmen seiner Managed-Database-Dienste automatische tägliche Backups. Die Aufbewahrungsfrist richtet sich nach dem gebuchten Support-Level und beträgt derzeit 7 Tage. * Der Auftragnehmer hat keinen direkten Zugriff auf diese infrastrukturseitigen Backups; * deren Verwaltung erfolgt ausschließlich durch diesen Unterauftragsverarbeiter gemäß dessen DPA. * Diese Backups werden nach Ablauf der Aufbewahrungsfrist regulär automatisiert überschrieben oder gelöscht.

12.5 Laufende Löschung während der Vertragslaufzeit Unabhängig von der Löschung nach Vertragsende löscht der Auftragnehmer die folgenden Bestände automatisiert, ohne dass es einer Weisung bedarf: * **Lernstände aus eingebetteter Nutzung ohne persönliche Anmeldung:** 270 Tage nach der letzten Aktivität der jeweiligen pseudonymen Lernidentität. Die Frist rechnet ab der letzten Aktivität und nicht je Aufgabe, damit einem aktiven Lernenden nicht während eines laufenden Kurses der Anfang entfällt. * **Verläufe der dialogbasierten Lernbausteine:** 270 Tage ab dem Zeitpunkt der einzelnen Nachricht.

Die Läufe erfolgen täglich. Der Auftraggeber kann eine kürzere Frist verlangen; eine längere Frist bedarf einer gesonderten Vereinbarung.

Erfolgt der Zugriff über eine in ein Fremdsystem eingebettete Komponente ohne persönliche Anmeldung, bildet der Auftragnehmer aus der Kennung des einbettenden Systems und der dortigen Nutzerkennung einen kryptografischen Streuwert. Gespeichert wird ausschließlich dieser Wert. Eine Zuordnung zu einer natürlichen Person ist dem Auftragnehmer ohne Mitwirkung des Auftraggebers nicht

möglich; für Auskunfts- und Löschersuchen bildet der Auftragnehmer den Streuwert aus einer vom Auftraggeber benannten Nutzerkennung und kann den Bestand gezielt ausgeben oder löschen.

13. Kontrolle und Auditrechte

Der Auftraggeber ist berechtigt, die Einhaltung dieser Vereinbarung sowie der gesetzlichen Datenschutzanforderungen durch den Auftragnehmer zu überprüfen. Audits erfolgen grundsätzlich als Dokumentenprüfung. Hierzu gehören insbesondere Einsicht in das TOM-Dokument, Datenschutzkonzepte, Sicherheitsmaßnahmen sowie Zertifizierungen oder Sicherheitsberichte der in der Anlage geführten Unterauftragsverarbeiter. Audits erfolgen remote und nur nach vorheriger schriftlicher Ankündigung mit angemessener Frist. Ein physischer Zugang zu Systemen, Servern oder Rechenzentren wird nicht gewährt. Der Auftragnehmer ist verpflichtet, auf Anfrage des Auftraggebers angemessene Informationen zur Verfügung zu stellen, soweit diese zur Bewertung der Datenschutzkonformität notwendig sind. Geschäftsgeheimnisse, sicherheitskritische Details oder interne Abläufe müssen nicht offengelegt werden. Der Umfang, die Dauer und der Zeitpunkt eines Audits dürfen den Geschäftsbetrieb des Auftragnehmers nicht unangemessen beeinträchtigen. Außerordentliche, besonders aufwändige Audits oder externe Prüfungen sind separat zu vereinbaren und können dem Auftraggeber in Rechnung gestellt werden.

14. Haftung

Für den Ersatz von Schäden, die ein Nutzer oder Dritte durch die Nutzung der Plattform erleiden, haftet der Auftragnehmer unbeschränkt nur bei Vorsatz oder grober Fahrlässigkeit. Für leichte Fahrlässigkeit haftet der Auftragnehmer nur bei Verletzung einer wesentlichen Vertragspflicht (Kardinalpflicht), deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber vertrauen darf. In diesem Fall ist die Haftung auf den bei Vertragsschluss vorhersehbaren, vertragstypischen Schaden begrenzt. Die Haftung für Datenverlust wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und gefahrensprechender Anfertigung von Sicherungskopien durch den Auftraggeber eingetreten wäre. Soweit der Schaden durch einen Unterauftragsverarbeiter (z. B. KI-Anbieter) verursacht wurde, tritt der Auftragnehmer vorrangig seine eigenen Schadensersatzansprüche gegen den Unterauftragsverarbeiter an den Auftraggeber ab. Eine subsidiäre Haftung des Auftragnehmers gemäß Art. 28 DSGVO bleibt hiervon unberührt.

15. Schriftform

Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieser Schriftformklausel. Elektronische Signaturen (z. B. DocuSign, Adobe Sign) sind zulässig und der handschriftlichen Unterschrift gleichgestellt. Anpassungen aufgrund gesetzlicher oder regulatorischer Änderungen dürfen vom Auftragnehmer schriftlich mit angemessener Frist angekündigt werden.

16. Schlussbestimmungen

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Im Falle von Widersprüchen zwischen dieser AVV und dem Hauptvertrag hat diese AVV Vorrang, soweit es um datenschutzrechtliche Regelungen geht. Individuell zwischen den Parteien getroffene und von beiden Seiten unterzeichnete Vereinbarungen – insbesondere eine gesonderte Nebenabrede zu dieser Vereinbarung – gehen den Bestimmungen dieser Vereinbarung vor, auch in datenschutzrechtlichen Fragen, soweit sie den Anforderungen des Art. 28 DSGVO genügen. Eine solche Nebenabrede benennt die Bestimmungen, die sie ersetzt oder ergänzt. Diese Vereinbarung unterliegt deutschem Recht. Gerichtsstand ist Darmstadt. Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft und gilt für die gesamte Dauer der Nutzung der Plattform.